МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ФІЛОЛОГІЇ ТА МАСОВИХ КОМУНІКАЦІЙ
КАФЕДРА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

До захисту допустити:
Завідувач кафедри
_____Кудлай В.О.
«11» травня 2026 р.

«СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ НА СУЧАСНОМУ ПІДПРИЄМСТВІ: ІНСТРУМЕНТИ ТА ТЕХНОЛОГІЇ»

Кваліфікаційна робота
здобувача вищої освіти бакалаврського
рівня вищої освіти, освітньо-професійної програми
«Документознавство, керування документаційними процесами»
Турсунов Гусейн

Науковий керівник:
Федотова Оксана Олегівна,
доктор історичних наук,
професор кафедри інформаційної діяльності
Рецензент:
Політова Олена Аркадіївна,
кандидат історичних наук,
завідувачка кафедри інформаційних комунікацій
Київського університету імені Бориса Грінченка

Кваліфікаційна робота захищена
з оцінкою добре 77С
Секретар ЕК_____
«12» червня 2026 р.

Київ – 2026

ЗМІСТ

ВСТУП

Актуальність дослідження. Відмінною рисою сучасності є глобальний перехід від індустріального суспільства до інформаційного, в якому головним стратегічним ресурсом стає інформація. Власне інформаційна сфера, що являє собою специфічну галузь діяльності суб'єктів суспільного життя, пов'язану зі створенням, зберіганням, розповсюдженням, передачею, обробленням і застосуванням інформації, є однією з базових складових сучасного суспільства будь-якої держави, що розвивається.

Швидке вдосконалення інформатизації та її проникнення у напрями життєво важливих інтересів зумовили, крім безперечних переваг, появу низки стратегічних проблем. Зокрема, суттєво посилюється небезпека несанкційонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем. Проникаючи в усі сфери діяльності суспільства і держави, інформація набуває конкретних політичних, матеріальних і вартісних виразів. Захист інформації як сукупність заходів, спрямованих на запобігання порушенню конфіденційності, цілісності, доступності даних та здійсненню їх несанкціонованої модифікації, стає пріоритетним завданням для забезпечення стабільного функціонування будь-якого сучасного підприємства.

Правове регулювання суспільних відносин, що виникають в інформаційній сфері, виступає пріоритетним напрямком процесу нормотворчості в Україні, метою якого є забезпечення інформаційної безпеки держави та суб'єктів господарювання відповідно до вимог законів України «Про інформацію», «Про державну таємницю» та «Про захист інформації в інформаційно-комунікаційних системах».

Проте динамічний розвиток методів маскування умисних загроз під випадкові збої, виклики євроінтеграції, поширення вірусів-вимагачів та потреба забезпечення юридичної сили документів вимагають постійного

вдосконалення систем захисту електронного документообігу, що й зумовлює актуальність обраної теми бакалаврської роботи.

Об’єкт дослідження – система захисту інформації на сучасному підприємстві.

Предмет дослідження – організаційно-правові та програмно-технічні механізми захисту електронного документообігу підприємства.

Мета дослідження полягає у висвітленні комплексу організаційно-технічних інструментів і апаратно-програмних технологій захисту інформації для побудови ефективної системи безпеки електронного документообігу на сучасному підприємстві.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1) визначити роль інформації як стратегічного ресурсу та розкрити специфіку інформаційної сфери в умовах сучасного суспільства;

2) з’ясувати сутність електронного документообігу у контексті криптографічного захисту інформації;

3) охарактеризувати нормативно-правову базу, завдання головних регуляційних інституцій та принципи нормотворчості у сфері забезпечення інформаційної безпеки України;

4) показати вплив євроінтеграційних процесів та стандартів (GDPR) на практику захисту даних в Україні;

5) охарактеризувати сучасні вірусні загрози для електронного документообігу та класифікувати методи їх подолання;

6) провести моделювання профілю порушника та класифікувати ризики несанкціонованого доступу до документованої інформації;

7) здійснити моніторинг уразливостей ІТ-інфраструктури ТОВ «ІнфоТех-Консалтинг»;

8) проаналізувати стан апаратно-програмного забезпечення безпеки інформаційної діяльності ТОВ «ІнфоТех-Консалтинг»;

9) окреслити напрямки модернізації системи захисту документаційної діяльності та перспективи автоматизації електронного документообігу підприємства.

Стан наукової розробленості теми. Вивченням зазначеної проблеми займалося чимало українських та зарубіжних вчених. У працях Б. Кормича та Є. Рогової багатоаспектно висвітлено загальнотеоретичні та організаційно-правові засади забезпечення державної інформаційної політики, правової інфраструктури та кібербезпеки [27; 55]. Питанням технічного, нормативного та методологічного захисту відомостей в автоматизованих мережах присвячені ґрунтовні наукові розробки К. Бєлякова та І. Босак [6; 8]. Практичні аспекти практичного застосування криптографічних засобів та побудови безпечного інформаційного середовища установ детально розкрито у посібниках О. Єсіна, О. Кузнецова та Л. Сороки [17] та ін.

Водночас, незважаючи на наявність значного масиву профільних наукових публікацій, пришвидшена еволюція кіберзагроз, стрімке поширення агресивних вірусів-вимагачів, а також специфіка імплементації жорстких європейських регламентів (GDPR) у щоденну практику діловодства України потребують подальшого комплексного аналізу. Вказані чинники підтверджують недостатню висвітленість прикладних аспектів організації безпеки в системах електронного документообігу (СЕД) на підприємствах, що й зумовило необхідність наукової розробки заявленої тематики дослідження.

Джерельну базу дослідження сформували: періодичні (наукові журнали з документознавства та кібербезпеки), неперіодичні (монографії, навчальні посібники, глосарії), а також продовжувані видання (матеріали міжнародних науково-практичних конференцій та збірники наукових праць). Важливими інформаційними джерелами для написання бакалаврської роботи стали законодавчі та нормативно-правові акти України, нормативні документи з технічного захисту інформації, а також європейські регламенти у сфері захисту персональних даних. Відповідно до функціонального

призначення використані нами матеріали можна розподілити на чотири основні групи: наукові, правові, навчальні та довідково-енциклопедичні.

У роботі застосовано комплекс наукових **методів**:

1) джерелознавчого аналізу (для формування джерельної бази роботи);

2) системний (для вивчення ІТ-інфраструктури);

3) метод моделювання загроз (для створення профілю порушника та класифікації ризиків несанкціонованого доступу до інформації на підприємстві);

4) порівняльний аналіз (при розгляді апаратно-програмних засобів захисту);

5) абстрагування (для зосередження на основних характеристиках захисту документа);

6) теоретичного узагальнення (для формулювання висновків).

Практичне значення отриманих результатів полягає у тому, що їх можливо застосувати для:

1) підготовки у профільних закладах вищої освіти навчальних курсів за напрямом спеціальності;

2) розробки конкретних рекомендацій щодо технічного, програмного та організаційного переоснащення систем електронного документообігу та захисту цифрових архівів сучасного підприємства;

3) оптимізації роботи діловодних та архівних служб за допомогою спроєктованого на прикладі діяльності ТОВ «ІнфоТех-Консалтинг» контуру апаратно-програмної безпеки.

Апробація результатів роботи та публікації. За результатами дослідження підготовлено такі тези доповідей:

1) Tursunov G. Systemic threats in the context of the accelerated digitalization of society (Системні загрози в умовах прискореної інформаизації суспільства). Science in the Context of Modern Challenges and Prospects: Proceedings of the II International Scientific Conference (Utrecht, Netherlands, 28 May 2026). Bookmundo, 2026. (подано до оргкомітету).

2) Турсунов Г. Вплив євроінтеграційних процесів на захист даних та електронний документообіг в Україні. III Міжнародна науково-практична конференція «Трансформаційні процеси соціально-гуманітарної освіти сучасної України в умовах війни: виклики, проблеми та перспективи» (Тернопіль, 23–25 червня 2026 р.). Тернопіль: Університетська думка, 2026. (подано до оргкомітету).

3) Федотова О., Турсунов Г. Специфіка електронного документообігу як об’єкта інформаційної безпеки. XI Міжнародні науково-практична конференція «Інформація та соціум» (Вінниця, 4-5 червня 2026). Вінниця: Донецький національний університет імені Василя Стуса, 2026. (подано до оргкомітету).

Структура дипломної роботи обумовлена її метою та завданнями дослідження. Кваліфікаційна праця складається зі вступу, трьох розділів, висновків, списку використаних джерел та літератури.

Загальний обсяг роботи становить 59 сторінок. Основний текст налічує 49 сторінок, список використаних джерел налічує 63 позиції.

РОЗДІЛ 1.
ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

1.1. Інформаційне суспільство, процеси управління та роль інформації як стратегічного ресурсу

Еволюція постіндустріального світу призвела до становлення глобального інформаційного суспільства, під яким розуміють новий, більш високий щабель розвитку людського соціуму, де переважна більшість працюючих осіб займається створенням інформаційних даних та знань, їх зберіганням, обробкою та використанням, а новітні інформаційно-комунікаційні технології виступають головним підґрунтям життєдіяльності суспільства [61]. В інформаційному суспільстві навички управління даними визначають успішність функціонування будь-якої організації. У цих нових реаліях інформаційний потенціал є центральним показником розвитку, а самі відомості набули ознак самостійного, стратегічного та товарного ресурсу. Зростання ролі інформації у функціонуванні сучасних установ вимагає від фахівців з документознавства формування якісних систем інформаційного менеджменту, які здатні забезпечити ефективний обіг відомостей всередині організацій та захистити їх від зовнішніх деструктивних впливів [32].

В Україні останнім часом відбуваються якісні зміни у процесах управління на всіх рівнях (від великих державних інституцій до приватних фірм). Ці глибокі трансформації безпосередньо зумовлені інтенсивним упровадженням новітніх інформаційних технологій. Зараз важко собі уявити підприємство чи компанію, яка з легкістю може обходитися без персональних комп’ютерів та відповідного програмного забезпечення [60]. Вже неможливо тримати всю інформацію в голові або на папері, тому комп’ютерні технології та автоматизовані системи електронного документообігу (СЕД) мають таку велику цінність для бізнесу. Обчислювальна техніка направлена на допомогу людству, вона оптимізує

витрати ресурсів, забезпечує високу швидкість обміну даними та гнучкість бізнес-процесів, але разом з необмеженими можливостями інноваційні технології приносять і нові проблеми [31].

Сучасні управлінські процеси на українських підприємствах та в органах влади зараз активно модернізуються, що прямо пов’язано з переходом на цифрові технології. Використання ERP та CRM-систем, технологій хмарних обчислень, можливостей впровадження систем електронного документування (СЕД) та засобів бізнесової аналітики перетворилося на важливу частину щоденної інформаційної діяльності підприємців [37].

Автоматизація та цифровізація управлінських процесів дозволили суттєво підвищити швидкість прийняття рішень, мінімізувати вплив людського фактора, оптимізувати витрати ресурсів та забезпечити гнучкість бізнес-процесів у мінливих ринкових умовах [60]. Інформаційні технології сьогодні виступають головним інструментом гарантування ефективного управління організаціями.

Проте швидке вдосконалення процесів інформатизації, розширення мережевої інфраструктури підприємств та проникнення цифрових інструментів в усі сфери життєво важливих інтересів зумовили, крім безперечних і очевидних переваг, появу низки серйозних стратегічних проблем. Головна з них полягає у тому, що із зростанням обсягів інформації, яка циркулює у корпоративних мережах, паралельно посилюється небезпека несанкційонованого втручання в роботу комп’ютерних, інформаційних і телекомунікаційних систем підприємства. Стрімке накопичення інформаційних масивів без належного контролю призводить до явища «інформаційного перевантаження», в умовах якого стає значно важче виявляти цілеспрямовані деструктивні впливи та аномалії у поведінці користувачів мережі [5].

Сучасне підприємство функціонує в умовах високої концентрації можливих цифрових ризиків. Інформаційні відомості, які зберігається в

актуальних базах даних організації (будь то комерційна таємниця, персональні дані клієнтів цільової аудиторії, матеріали фінансової звітності, документи поточного та перспективного планування), характеризуються високою ціною. Їхня втрата, спотворення або несанкційоноване оприлюднення може призвести не лише до прямих фінансових збитків чи юридичної відповідальності, але й до повної руйнації ділової репутації певної компанії, втрати ринкових позицій та навіть банкрутства [5]. Більше того, у масштабах держави інформаційна безпека окремих суб'єктів господарювання (у першу чергу, підприємств критичної інфраструктури, енергетичного сектору, логістики) безпосередньо впливає на економічні, соціальні та оборонні аспекти життєдіяльності країни [47; 53].

Варто зазначити, що інформаційна діяльність сучасного підприємства потребує безперервного моніторингу та оцінки ризиків. Документована інформація виступає основою для прийняття будь-яких управлінських рішень, тому її якість повнота і точність визначають ефективність роботи всієї організації [31]. У випадку компрометації інформаційних потоків або порушення конфіденційності стратегічних документів, підприємство втрачає функціональну стабільність, що підтверджує необхідність створення комплексного організаційно-правового та технічного периметрів захисту [54]. У цьому контексті важливим є врахування міжнародних стандартів та інформаційної політики Європейського Союзу у сфері регламентації прав та безпеки суб'єктів в Інтернет-середовищі [59], де базові термінологічні рамки [61] стають орієнтиром для побудови корпоративних систем кіберзахисту [42].

Таким чином, організація ефективного захисту інформаційних ресурсів потребує системного підходу, що зумовлює комплексне використання нормативно-правових, організаційні, програмно-апаратних засобів, детальному аналізу яких присвячено наступні розділи цього дослідження.

1.2. Сутність електронного документообігу у контексті криптографічного захисту інформації

Цифровий перехід сучасних підприємств до автоматизованого провадження діловодної справи потребує докладного аналізу властивостей цифрового документа та конкретизації основних інструментів, що можуть засвідчувати його автентичність. Слід зазначити, що організація фахово захищеної інформаційної діяльності організації напряму ґрунтується на усвідомленні особливостей обігу електронних даних та застосуванні надійних інструментів задля їхньої збереженості. Зважаючи на те, що електронний документ напряму зазнає впливу різного роду технологічних факторів у процесі передачі відкритими мережами, сутнісний аспект операцій документообігу на сучасному етапі розглядається паралельно з технологічною специфікою криптографічних перетворень та урахуванням наявної інфраструктури довірчих послуг.

Слід уточнити дефініцію «електронний документообіг». Під нею мають на увазі комплекс операцій зі створення, обробки, надсилки, транспортування, передачі, отримання, зберігання, застосування та кінцевого знищення електронних документів, що виконуються із паралельним провадженням перевірки їхньої цілісності та у випадку потреби підтвердити факт надходження та одержання такого роду документів [44]. Для фахівців галузі документознавства та архівної справи впровадження ЕДО означає концептуальну зміну підходів до збереження інформації, організації інформаційної діяльності та корпоративного управління [4].

Специфіка електронного документообігу як об’єкта інформаційної безпеки полягає у фізичній нематеріальності цифрового документа. На відміну від паперового носія, де інформація жорстко прив’язана до матеріалу (паперу, чорнила), електронний документ – це структурований набір двійкових даних. Це породжує низку унікальних загроз, які вимагають специфічних методів захисту. Найбільш критичною з таких загроз є

несанкційонований доступ (НСД) – тобто, одержання доступу до актуальних інформаційних ресурсів певними суб'єктами особами чи процесами без відповідних офіційних повноважень [34]. Захист електронного документообігу традиційно розглядається через забезпечення класичної тріади інформаційної безпеки, яка безпосередньо адаптується під потреби сучасного діловодства [11]:

1. Конфіденційність – гарантія того, що зміст електронного документа (особливо з грифом «Комерційна таємниця» або «Для службового користування») буде доступний лише авторизованим користувачам.

2. Цілісність – забезпечення того, що електронний документ не був випадково або навмисно змінений, доповнений чи частково знищений у процесі його передачі корпоративною мережею або під час зберігання на сервері архіву.

3. Доступність – гарантія того, що легітимний користувач (наприклад, діловод або керівник установи) зможе отримати своєчасний і безперешкодний доступ до необхідного документа в базі даних.

Окремим, вкрай важливим атрибутом для систем ЕДО є автентичність – здатність довести, що автором документа є саме та особа, яка під ним підписалася, і що документ дійсно був створений у зазначений час. Без гарантування цих властивостей електронний документообіг втрачає будь-яку юридичну силу та перетворюється на вразливу мішень для зловмисників [23].

Головною вимогою щодо захисту інформації відкритого типу є збереження її цілісностного стану, що досягається за допомогою організації захисту даних від несанкційонованих дій, що здатні спричинити їхню випадкове чи навмисне спотворення, модифікацію або ж навіть знищення. Тому з урахуванням дотримання встановленого режиму доступу до таких інформаційних даних:

1) абсолютно усім потенційним користувачам має бути гарантований безперешкодний доступ до ознайомлення з відкритими відомостями;

2) спотворення чи знищення відкритих даних може провадитися виключно тими користувачами, які наділені такими правовими повноваженнями;

3) будь-які намагання модифікувати або ж знищити відкриту інформацію особами, які офіційно не мають на це права, повинні припинятися шляхом блокування сторонніх дій [11].

У свою чергу гарантування дотримання спеціального режиму доступу до таємних або конфіденційних даних включає наступні вимоги:

- надання доступу до конфіденційної інформації дозволяється надається виключно користувачам з відповідними повноваженнями;
- намагання доступу до вказаної інформації сторонніх користувачів, без відповідних повноважень, мають одразу ж бути припинені та блокуватися;
- певному користувачеві може дозволятися виконання однієї або декількох чітко окреслених операцій з оброблення конфіденційних даних або ж за потреби він позбавляється даного права.

Характерними різновидами такого роду неправомірних дій під час інформаційної діяльності на підприємстві є:

1) проведення процесу ознайомлення з конфіденційними даними різноманітними способами, але без порушень їх структури та цілісності;

2) зміна інформації з незаконною метою або як часткова чи загальна модифікація її складу;

3) цілеспрямоване знищення даних задля завдання матеріальних збитків.

Наслідком неправомірних дій з даними стає порушення їх конфіденційного характеру, повноти, достовірності фактажу та доступності, що у кінцевому результаті спричиняє порушення як самого режиму управління інформацією, так і його якісного боку за умов спотворення даних або ж їх неповноти [1].

Важливим аспектом дослідження є забезпечення ефективного збереження інформації, для чого потрібно застосовувати цілий комплекс інструментів. Як зазначає О. Нестеренко, для ефективного захисту документованої інформації необхідно застосовувати комплексний підхід, що об’єднує програмно-апаратні засоби, організаційні заходи та спеціальні математичні методи цілеспрямованого перетворення даних, які повністю виключають можливість їх прочитання сторонніми користувачами [33].

В умовах масового використання відкритих каналів зв’язку та Інтернету для обміну електронними документами суто організаційних і технічних заходів периметрального захисту виявляється недостатньо. У науковій літературі окремо розглядаються криптографічні методи захисту інформації та загальна технологія шифрування як найбільш надійний засіб протидії несанкціонованому доступу та перехопленню даних [1, с. 44]. Криптографічний захист перетворює інформацію електронного документа на незрозумілий шифротекст, роблячи його абсолютно марним для зловмисника, який не володіє правильним ключем дешифрування. Сучасна криптографія вирішує завдання не лише забезпечення конфіденційності, а й цілісності даних та автентифікації сторін [23, с. 10].

Варто зауважити, що у теорії захисту інформації для гарантування правової сили та збереження автентичності двійкових даних вирішальну роль відіграє асиметричне шифрування, більш відоме як криптографія з відкритим ключем. Математичне підґрунтя асиметричної криптографії базується на використанні пари пов’язаних між собою ключів: відкритого та закритого (оперсонального), де один ключ застосовується для перетворення відомостей, а інший – навпаки, для їхнього зворотного відновлення [23].

Основою для перевірки стану незмінності певного тексту в цифровому просторі вважається математична функція хешування, за допомогою якої вихідний масив документа перетворюється в унікальний рядок символічних знаків фіксованої довжини (хеш-код або дайджест). Причому, будь-яка зміна хоча б одного знака докорінно змінює цей дайджест, що закладає теоретичну

базу для перевірки цілісності актуальних даних [10]. На підставі того досягається високий рівень захищеності документа.

Отже, криптографічні методи захисту електронного документообігу на сьогодні є чи не найнадійнішими.

1.3. Нормативно-правова база України та завдання державних інституцій у сфері технічного захисту інформації

Побудова будь-якої системи захисту інформації та забезпечення безпеки електронного документообігу на підприємствах неодмінно спирається на чіткий законодавчий фундамент [27]. Державна політика України у цій сфері покроково формується з максимальним урахуванням необхідності дотримування балансу між конституційним правом осіб на інформацію, свободою підприємницької діяльності та обов'язком держави захищати чутливі, стратегічно важливі дані від актуальних зовнішніх і внутрішніх загроз. Саме тому забезпечення інформаційної безпеки держави є однією з найважливіших функцій.

Нормативно-правовий характер регулювання діючих суспільних відносин, які мають місцк в інформаційній галузі, стає визначальним вектором нормотворчого процесу, пріоритетною метою якого виступає формування безпечного, захищеного цифрового простору для забезпечення безперешкодної діяльності органів державної власти, а також осіб-підприємців в установах усіх форм власності [24].

Базовими нормативно-правовими актами, що детально регулюють питання захисту електронних документів, визначають правовий статус цифрових архівів та встановлюють вимоги до технічного захисту інформації (ТЗІ), є: Закони України «Про інформацію», «Про електронні документи та електронний документообіг», «Про електронну ідентифікацію та електронні довірчі послуги», «Про захист інформації в інформаційно-комунікаційних

системах» тощо. Кожен із них закладає окрему правову цеглинку в загальну архітектуру безпеки ЕДО.

Закон України «Про інформацію» пропонує семантичну основу захисту, розподіляючи всі інформаційні дані на відкриті та з обмеженим доступом (конфіденційні, таємні, службові). Саме ця класифікація є першочерговою для документознавців при формуванні номенклатури справ, а також у процесі визначенні рівня доступу працівників до електронних папок.

Фундаментальне значення для побудови цифрових систем автоматизації бізнесу має Закон України «Про електронні документи та електронний документообіг». Він закріплює правовий статус електронного документа, підносячи його за юридичною дією до паперового еквівалента, а також чітко регламентує життєвий цикл цифрового документа від моменту його створення до фінального архівного знищення [42].

Своєю чергою, Закон «Про захист інформації в інформаційно-комунікаційних системах» регламентує жорсткі імперативні вимоги до технічного аспекту обігу документів [46]. Відповідно до його норм, оброблення інформації з обмеженим доступом в електронному вигляді в державних та деяких корпоративних мережах категорично заборонена без створення Комплексної системи захисту інформації (КСЗІ), що потребує підтвердження відповідним атестатом державного зразка відповідності, наданим Державною службою спеціального зв’язку та захисту інформації України. В українській практиці еталоном інтеграції організаційних та інженерно-технічних заходів є саме КСЗІ, яка за нормативними документами (НД ТЗІ) становить собою взаємопов’язаний комплекс інструментів, засобів і методичних прийомів захисту інформаційних даних [34].

Головним інституційним регулятором у цій сфері є Державна служба спеціального зв’язку та захисту інформації України (Держспецзв’язку) [39; 40]. Вона була створена на виконання прийнятого 23 лютого 2006 р. Закону України «Про Державну службу спеціального зв’язку та захисту інформації

України» на базі ліквідованого Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України, що визначалося на підставі Указу Президента України від 07.11.2005 № 1556/2005 «Про додержання прав людини під час проведення оперативно-технічних заходів». Цей указ окреслив потребу в утворенні центрального органу виконавчої влади зі спеціальним статусом для реалізації державної політики у сфері захисту державних інформаційних ресурсів.

Базовими задачами Держспецзв'язку України у галузі організації захисту наявних інформаційних ресурсів та діловодних систем є:

– гарантування розроблення і реалізації державної політики у галузях забезпечення захисту типових державних систем (інформаційних, телекомунікаційних та інформаційно-комунікаційних), основ крипто- та технічного захисту інформаційних даних, застосування і захищеності державних електронних інформаційних масивів документів, телекомунікаційних технологій, користування актуальними радіочастотними ресурсами держави;

– активна участь у розробці і провадженні державної політики у галузі електронного документування органів державної влади та місцевого самоврядування, створенні та застосуванні кваліфікованого електронного підпису (КЕП) у владних структурах;

– взяття участі відповідно до власних повноважень у розроблені та провадженні державної політики тарифного плану, а також стосовно закупівель у галузях телекомунікаційних технологій, використання радіочастотного ресурсного резерву;

– організація надання в офіційному порядку урядового зв'язку Президентові України, Голові ВР, Прем'єр-міністрові, уповноваженим особам органів державної влади, представникам місцевого самоврядування, профільним органам військового управління, очільникам різного роду установ у мирний час, за умов введення надзвичайного та воєнного стану, а також за потреби, при запровадженні надзвичайної ситуації;

– надання допомоги в організації належної роботи, безпеки та всебічного розвитку державної комплексної системи урядового зв'язку, а також у функціонуванні Національної системи конфіденційного зв'язку країни;

– окреслення вимог і визначення порядку створення й розвитку базових систем технічного та криптографічного захисту інформаційних даних, що вважаються державною власністю, чи інформації з обмеженим доступом, потреба стосовно захисту якої прописана законодавчо;

– проведення багатоаспектного державного контролю за станом крипто- та технічного захисту інформаційних даних, що є державною власністю, чи інформації обмеженого характеру, потреба у захищенні якої закріплена на законодавчому рівні, запобіганні здійсненню технічних розвідок, додержанні технічних вимог управлінської документації у галузі надання кваліфікованих послуг щодо проставляння електронного підпису;

– підтримка та участь в охороні профільних об'єктів та майна Управління Держспецзв'язку України, фізичних приміщень, інформаційних систем, мережевих комплексів, засобів налагодження безперебійного урядового і спеціального зв'язку, документації щодо криптографічних засобів захищеності даних тощо;

– розробка та проведення заходів стосовно питань розвитку телекомунікаційних технологій, покращення їхньої якості, гарантування доступності й безперебійної роботи;

– забезпечення інтегрованості телекомунікаційних засобів, використання радіочастотного ресурсу держави у зарубіжний інформаційний та комунікаційний простір [39].

Одним із найпріоритетніших та стратегічно важливих завдань Держспецзв'язку є забезпечення функціонування, безпеки та розвитку Національної системи конфіденційного зв'язку (НСКЗ), активні роботи з побудови якої були започатковані у 2002 р. на виконання Закону України «Про Національну систему конфіденційного зв'язку» [50]. Безпосередню

реалізацію вказаних функцій покладено на Департамент стратегії розвитку спеціальних інформаційно-телекомунікаційних систем, Департамент безпеки інформаційно-телекомунікаційних систем та Державне підприємство «Українські спеціальні системи» (ДП «УСС»).

У контексті нашої теми дослідження слід приділити увагу характеристиці Національної системи конфіденційного зв'язку. Вона являє собою цілісну єдність спеціалізованих систем/мереж зв'язку, що характеризуються подвійним призначенням, які шляхом застосування крипто- чи технічних інструментів здійснюють якісний обмін конфіденційними даними, виходячи з інтересів органів державної влади та місцевого самоврядування, закладають необхідні умови задля їх максимальної взаємодії як у мирний час, так і у випадку оголошення надзвичайної ситуації. Абонентами цієї системи можуть бути як державні, так і комерційні структури, юридичні та фізичні особи, суб'єкти фінансово-економічної сфери [6]. Уточнимо, що принцип подвійного призначення полягає у тім, що в мирний час мережі використовуються організаціями для передачі сучасними видами зв'язку конфіденційних даних, а в особливий період ресурс повністю задіюється для потреб національної безпеки та оборони держави.

Впровадження НСКЗ провадиться відповідно до положень Державної цільової програми. Це дозволяє забезпечити надійний захист конфіденційної інформації, створити передумови для успішної інтеграції розподілених інформаційних ресурсів та аналітичних систем органів влади різного рівня управління та налагодити між ними надійну інформаційну взаємодію. Послуги в НСКЗ реалізуються із забезпеченням необхідного рівня захисту. Так, здійснюється [53]:

1) шифрування інформації за допомогою засобів криптографічного захисту (КЗХІ);
2) резервування критичного обладнання та каналів;
3) цілодобовий контроль за функціонуванням системи;

4) блокування розповсюдження комп'ютерних вірусів;

5) забезпечення швидкої реакції на спроби неправомірного доступу.

До складу НСКЗ входить транспортна (телекомунікаційна) мережа, спеціальні мережі надання послуг стаціонарного та мобільного зв'язку, централізована система захисту інформації та централізована система оперативно-технічного управління. Першою чергою створення НСКЗ став розвиток мережі у м. Києві, де на сьогодні розгорнуто 38 вузлів зв'язку, побудовано близько 100 кілометрів волоконно-оптичних ліній зв'язку та створено Технічний центр, до складу якого входить головний вузол зв'язку НСКЗ та центр технічного управління. Ця інфраструктура вже забезпечує функціонування систем, в яких циркулює інформація з обмеженим доступом (наприклад, Системи діловодства та контролю виконання доручень Кабінету Міністрів України), а також відкриті ресурси (Єдиний веб-портал органів виконавчої влади).

Ресурс НСКЗ задіяно в Єдиній державній інформаційній системі у сфері запобігання та протидії легалізації доходів, одержаних злочинним шляхом [44], аналітичному центрі Міжвідомчої координаційної ради з питань боротьби з контрабандою [45] та проєкті БУМАД 2 в рамках Програми Розвитку ООН (ПРООН).

З аналізу чинного законодавства та підзаконних нормативних актів можна зробити узагальнення, що в Україні створена дієва національна система правового регулювання захисту інформації в автоматизованих системах.

Правову основу забезпечення захисту інформації в Україні як інституції права становлять Конституція України, закони України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про державну таємницю», «Про науково-технічну інформацію», інші нормативно-правові акти, в тому числі численні міжнародні договірні акти України, що мають відношення до галузі інформаційних взаємовідносин.

Проте, критичний підхід щодо аналізу Концепції технічного захисту інформації, як нормативно-правового акта (документа) свідчить про невідповідність його назви (форми) та змісту [55]. По суті, цей документ являє собою не систему, а звичайну сукупність норм. У ньому йдеться не стільки про організацію інженерно-технічного захисту (організаційно-технічні заходи), скільки про організаційно-управлінські та організаційно-правові заходи [6].

Незважаючи на наявність розгалуженої нормативної бази, українські дослідники вказують на існуючі проблеми. Як зазначає Є. Рогова, у законодавчому полі України, на жаль, відсутній єдиний рамковий закон щодо інформаційної безпеки держави, а чинне законодавство потребує вдосконалення базових термінологічних положень [55, с. 190]. Розпорошеність норм між різними законами та підзаконними актами іноді створює колізії на практиці, ускладнюючи роботу фахівців із захисту інформації в установах. Вирішенням цієї проблеми могла б стати кодифікація законодавства – розробка та прийняття Інформаційного кодексу України.

Висновки до розділу 1

1) У сучасному інформаційному соціумі інформація видозмінилася з виключно додаткового засобу фіксації даних на автономний, незалежний та достатньо вразливий, проте вкрай необхідний ресурс. Ефективна технологічна модернізація основних систем управління на базі IT-технологій потребує превентивного, заздалегідь продуманого розвитку допоміжних інструментів захисту даних. Комплексна безпека інформаційного простору підприємства більше не є суто технічним завданням IT-відділу, а виступає базовою передумовою функціонального виживання та стратегічної стабільності будь-якої бізнес-структури.

2) Криптографічні перетворення інформації та інфраструктура відкритих ключів формують технологічну базу, на якій тримається довіра до

електронного документообігу в Україні, забезпечуючи його юридичну значущість та захищеність від підробки.

3) Нормативно-правова база України загалом забезпечує необхідне підґрунтя для функціонування та захисту електронного документообігу, проте потребує подальшої систематизації та адаптації до динамічних змін у кіберпросторі. Тематика захисту інформації в автоматизованих системах у науково-теоретичній і прикладній сферах України знаходиться на етапі формування, з приводу чого вимагає фахової систематизації, зокрема на організаційно-правовому рівні.

СТАН, ТЕНДЕНЦІЇ ТА КІБЕРЗАГРОЗИ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ ДІЯЛЬНОСТІ СУЧАСНИХ УСТАНОВ

2.1. Вплив євроінтеграційних процесів та міжнародних стандартів (GDPR) на практику захисту даних в Україні

Стрімка цифровізація інформаційного простору України, інтеграція суб'єктів господарювання у глобальне цифрове середовище та масовий перехід на хмарну інфраструктуру в умовах воєнного стану висувають нові вимоги до організації діловодства. Аналіз практики захисту електронного документообігу неможливий без урахування міжнародно-правового контексту. В умовах глобалізації інформаційного суспільства обрання Україною євроінтеграційного курсу зумовило подальший вектор її розвитку, дотримання якого вимагає виконання цілої низки суворих вимог. Пріоритетним завданням для української системи управління документацією є імплементація норм Європейського Союзу, де інформаційна політика формується з орієнтацією на максимальний захист прав користувачів та їхніх персональних даних. Задля забезпечення відповідності чинним європейським стандартам в інформаційній галузі Україні необхідно імплементувати ефективні інструменти, що зможуть найкращим чином сприяти реалізації прав користувачів інтернет-середовища [59].

Фундаментальною подією, яка докорінно змінила підходи до захисту інформації в корпоративних мережах та архівах усього світу, стало набрання чинності Загальним регламентом про захист даних (General Data Protection Regulation – GDPR) у травні 2018 р. Екстериторіальний принцип дії GDPR означає, що будь-яка українська компанія, державна установа чи архів, яка обробляє персональні дані громадян ЄС, зобов'язана дотримуватися цих європейських стандартів [36].

Введення стандартизованих правил GDPR на українську ниву електронного документування потребує обґрунтованого переходу до парадигми «Privacy by Design» (дотримання конфіденційності на стадії

проєктування) та «Privacy by Default» (урахування вимоги конфіденційності за замовчуванням). У межах інформаційної діяльності це означає, що захисні механізми мають закладатися в архітектуру системи ЕДО ще на стадії її розробки або вибору розробника, а при реєстрації нового користувача в системі за замовчуванням повинні виставлятися максимально жорсткі обмеження прав доступу до корпоративних папок [20]. На практиці це створює низку нових викликів та завдань для діловодів та фахівців з інформаційної безпеки:

1. Мінімізація даних. Установи більше не можуть збирати та архівувати інформацію «про всяк випадок». В електронних формах та базах даних має зберігатися лише той мінімум персональних даних, який критично необхідний для надання послуги чи виконання договору [57].

2. Право «бути забутим» (Right to be forgotten). Українські системи електронного документообігу (СЕД) повинні мати технічну можливість безповоротно видаляти всі сліди перебування особи в базах даних. Проте реалізація цього права в українському діловодстві часто вступає в правовий конфлікт із Законом «Про Національний архівний фонд та архівні установи», який заперечує знищення документів тривалого зберігання [49]. Варіантом вирішення цієї проблеми в СЕД стає технологія анонімізації (знеособлення) відомостей, коли персональні дані особи в тексті документа повністю стираються або кодуються, але сам документ і його реєстраційний індекс в системі залишаються недоторканими для збереження цілісності архівного фонду.

3. Аудит та повідомлення про витоки. За європейськими стандартами, у разі зламу сервера та витоку архівних даних, установа зобов'язана повідомити про це регулятора та самих суб’єктів даних протягом 72 годин від моменту виявлення проблеми [18].

В умовах швидкої цифровізації суспільства електронні документи стають основним носієм інформації в багатьох сферах діяльності. Вони забезпечують зручність, швидкість обробки та зберігання інформації, проте

разом із цими перевагами постають і нові виклики, пов’язані зі стандартизацією електронних документів. Аналізуючи проблеми, що виникають в цій сфері, можна виділити кілька ключових аспектів: зберігання, автентичність та захист електронних документів.

Однією з основних проблем у стандартизації електронних документів є їхнє зберігання. У сучасних умовах постійного зростання обсягу інформації, що створюється та зберігається в електронному вигляді, необхідно мати ефективні рішення для архівування документів. В Україні відсутня єдина система зберігання електронних документів, що ускладнює їхнє управління. Стандарти, такі як ДСТУ 2732:2023, надають рекомендації щодо організації зберігання електронних документів, проте їхня реалізація не завжди забезпечується в практиці [26]. Брак уніфікованих вимог до формату та структури електронних документів загрожує труднощами їх інтеграції в існуючі інформаційні системи. Необхідно також враховувати різноманітність електронних носіїв та платформ, що використовуються для зберігання документів, адже це може ускладнити доступ до інформації в майбутньому.

Актуальним викликом є також питання автентичності електронних документів. Оскільки електронні документи можуть бути легко змінені або підроблені, важливо забезпечити їхню цілісність та правоздатність. Для цього використовуються різноманітні методи підтвердження автентичності, такі як:

– цифрові підписи;

– електронні штампи часу;

– інші криптографічні засоби.

Міжнародні стандарти, наприклад, ISO 32000, що регулюють документи PDF, містять рекомендації щодо використання цифрових підписів для підтвердження автентичності. Проте в Україні питання автентичності електронних документів залишається недостатньо врегульованим на законодавчому рівні, що викликає сумніви у правоздатності таких документів у судових процесах. Це підкреслює необхідність розробки та

впровадження чітких стандартів для електронних підписів та їхньої інтеграції в існуючі системи електронного документообігу [16].

Захист електронних документів є ще одним важливим аспектом, що потребує уваги. В умовах постійних загроз кібербезпеці, таких як несанкціонований доступ, шкідливе програмне забезпечення та кібератаки, необхідно забезпечити надійний захист електронних документів. Міжнародні стандарти, зокрема ISO/IEC 27001, надають основи для управління інформаційною безпекою, включаючи захист електронних документів [15]. В Україні існують національні нормативи, які регулюють захист інформації, проте їхня імплементація в практиці часто є недостатньою. Відсутність чітких стандартів і методик захисту електронних документів призводить до підвищеного ризику втрати або компрометації важливої інформації. Це створює значні ризики для організацій, які обробляють чутливі дані, адже кібератаки можуть призвести не лише до втрати інформації, а й до фінансових втрат і шкоди репутації [3].

Проблема довгострокового зберігання електронних документів залишається актуальною через постійний розвиток технологій. Сучасні формати файлів та програмне забезпечення швидко змінюються, що може створити труднощі з доступом до документів через кілька десятиліть. Один із прикладів – старі версії форматів документів, наприклад, файли з текстовими редакторами, які вже не підтримуються сучасними програмами, що робить їх недоступними без спеціалізованих конверторів чи програмного забезпечення.

Існує також проблема старіння носіїв інформації. Наприклад, раніше широко використовувані носії, як-от дискети, сьогодні вже майже не застосовуються і стають непрактичними для зберігання. Це ставить під загрозу можливість відновлення даних із таких носіїв у майбутньому. Переходячи до хмарних технологій або спеціалізованих архівів даних, організації можуть зменшити ці ризики, проте і тут є потреба у стандартизації таких процесів [19].

Ще одним важливим аспектом є можливість міграції даних на нові технологічні платформи без втрати цілісності та автентичності документів. Цей процес передбачає постійне оновлення даних і перенесення їх на нові формати або носії, що вимагає наявності спеціалізованих інструментів і чітких стандартів. Крім того, при перенесенні документів на нові платформи слід враховувати забезпечення юридичної сили документів, особливо в контексті їх автентичності та цифрових підписів.

Використання відкритих стандартів, таких як PDF/A (спеціальний формат PDF для архівування), є одним із рішень для довгострокового зберігання електронних документів. Цей формат створений таким чином, щоб забезпечити доступність документів незалежно від змін у програмному забезпеченні чи технологіях. Він гарантує, що всі елементи документа, включаючи шрифти, зображення та інші компоненти, будуть збережені всередині файлу, забезпечуючи можливість відтворення документа в майбутньому без втрати важливих даних.

Важливим також є створення національних або міжнародних архівних програм, які могли б забезпечити централізоване та стандартизоване зберігання електронних документів. В таких архівах варто використовувати надійні методи резервного копіювання та захисту від кіберзагроз, а також передбачати регулярні перевірки цілісності даних. Це може значно зменшити ризики втрати цінної інформації через технічні або організаційні проблеми.

Для ефективного довгострокового зберігання електронних документів необхідно впроваджувати відкриті формати, розробляти стратегії міграції даних на нові технологічні платформи, забезпечувати їхній правовий статус, а також створювати архівні системи, які відповідають сучасним викликам інформаційної безпеки та технологічного розвитку [18].

Стандартизація електронних документів для довгострокового зберігання є визначальним елементом у забезпеченні доступності інформації через десятиліття. Сучасні технології постійно змінюються, тому без чітких стандартів існує високий ризик того, що документи, створені сьогодні,

будуть недоступні або пошкоджені в майбутньому. Впровадження міжнародних та національних стандартів, таких як PDF/A, дозволяє уникнути таких проблем, забезпечуючи збереження і можливість відтворення документів незалежно від змін у програмному забезпеченні чи інфраструктурі.

Важливою складовою є впровадження стратегій міграції даних на нові платформи, щоб уникнути їх застарівання. Це вимагає активної роботи як з боку розробників програмного забезпечення, так і від державних органів, що регулюють архівну діяльність. Паралельно з цим необхідно приділяти велику увагу інформаційній безпеці електронних документів, оскільки їх збереження в електронному вигляді робить їх вразливими для кібератак та несанкціонованого доступу. Довгострокове зберігання також вимагає відповідальності з боку організацій, які зберігають електронні документи, у впровадженні надійних систем резервного копіювання та захисту від втрати даних.

Таким чином, успішна стандартизація електронних документів сприяє не тільки збереженню важливої інформації, але й підвищенню ефективності роботи установ, захисту документів від втрат та забезпеченню правової спадковості даних у майбутньому.

2.2. Шкідливе програмне забезпечення як деструктивний чинник в системах електронного документообігу

Швидке вдосконалення інформатизації та її проникнення у напрями життєво важливих інтересів зумовили, крім безперечних переваг, появу низки стратегічних проблем. Незважаючи на вдосконалення нормативно-правової бази, технічний захист електронного документообігу та управління інформаційними ресурсами залишається процесом безперервної протидії кіберзлочинності. Широке впровадження комп’ютерів та автоматизованих систем у практику діловодства призвело до того, що загрози втрати,

модифікації або блокування конфіденційної інформації стали щоденною реальністю практично будь-якої управлінської діяльності [1].

Автоматизація та цифровізація управлінських процесів дозволили суттєво підвищити швидкість прийняття рішень, мінімізувати вплив людського фактора, оптимізувати витрати ресурсів та забезпечити гнучкість бізнес-процесів у мінливих ринкових умовах. Інформаційні технології сьогодні виступають головним інструментом забезпечення ефективного управління організаціями [60]. Проте розширення мережевої інфраструктури підприємств та проникнення цифрових інструментів в усі сфери життєдіяльності зумовили, крім безперечних і очевидних переваг, появу серйозних ризиків. Із зростанням обсягів інформації, яка циркулює у корпоративних мережах, паралельно посилюється небезпека несанкційонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем підприємства. Стрімке накопичення інформаційних масивів без належного контролю призводить до явища «інформаційного перевантаження», в умовах якого стає значно важче виявляти цілеспрямовані деструктивні впливи та аномалії у поведінці користувачів мережі [13].

Найбільш руйнівним інструментом у цій сфері сьогодні виступає шкідливе програмне забезпечення. Серед усього спектра цифрових загроз найбільшу небезпеку для електронних архівів та систем документообігу підприємств становлять програми-вимагачі (Ransomware). Вектор їхньої атаки спрямований не стільки на викрадення даних, скільки на їх повне криптографічне закриття (шифрування) з метою подальшого отримання викупу від власників інформаційного ресурсу. Механізм зараження найчастіше базується на методах соціальної інженерії та фішингу: працівник діловодної служби отримує електронного листа, замаскованого під офіційне звернення чи фінансовий рахунок, відкриття якого автоматично запускає прихований алгоритм деструктивного впливу [33].

Специфіка кіберзлочинності полягає в тому, що умисні загрози можуть маскуватися під випадкові шляхом довгочасної масованої атаки несанкційонованими запитами або комп'ютерними вірусами [1]. Наприклад, Ransomware здатні за лічені години зашифрувати сервери баз даних та довгострокові цифрові архіви установи, а сама атака може маскуватися під раптовий апаратний збір мережі. Для фірми, що внаслідок зловмисний дій позбулася доступу до своєї системи ЕДО, наслідки можуть бути незворотними та призвести до погіршення ефективності чи навіть суцільного унеможливлення управлінських операцій. Класичним прикладом ураження мереж України стала атака вірусу Petya/NotPetya протягом 2017 р., яка заблокувала роботу тисяч українських підприємств та державних органів саме через уразливості в контурі оновлення програмного забезпечення для звітності та документообігу.

Для надійного захисту та подолання цих сучасних загроз практика інформаційної діяльності в Україні вимагає обов'язкового застосування таких базових інструментів:

1. Сувора дисципліна резервного копіювання. Впровадження міжнародно визнаного «правила 3-2-1» для електронних архівів (створення трьох копій даних, на двох різних типах носіїв, одна з яких обов'язково зберігається фізично ізольовано поза межами підприємства). Це є єдиним надійним способом відновити документи без виплати викупу зловмисникам.

2. Технологічна сегментація мереж. Розподілення внутрішньої корпоративної інфраструктури на ізольовані підмережі. Комп'ютери працівників, які активно взаємодіють із зовнішнім інтернет-середовищем, не повинні мати безпосереднього адміністративного доступу до серверів зберігання баз даних СЕД.

3. Систематичне підвищення рівня кібергігієни співробітників. Систематична підготовка та здійснення спеціальних інструктажів для працівників діловодної служби та менеджерів з різних аспектів ідентифікації

та виявлення фішингових повідомлень та правил забезпечення безпечної роботи з вхідною документацією [11].

Як ми могли переконатися, сучасні вірусні загрози та атаки шкідливого програмного забезпечення на кшталт Ransomware створюють реальну небезпеку для стабільної роботи будь-якого підприємства, оскільки їхній вплив зорієнтований на руйнування або блокування стратегічно важливих цифрових масивів інформації. Намагання зловмисників завуальовувати умисно спрямовані кібератаки під суто технічні, випадкові апаратні проблеми надзвичайно ускладнює функціонування діловодних та інформаційно-аналітичних підрозділів, загрожуючи спотворити весь процесу операційного управління даними.

2.3. Моделювання профілю порушника та класифікація ризиків несанкційонованого доступу до документованої інформації

Відповідно до методології побудови комплексних систем захисту інформації (КСЗІ), наступним після загального аналізу інфраструктури критично важливим етапом є розробка моделі гіпотетичних загроз та моделі можливого порушника. Цей процес дозволяє чітко ідентифікувати потенційні джерела небезпеки, визначити вектори можливих атак на автоматизовані системи та оцінити наслідки їхньої реалізації для безперервності інформаційної діяльності й операційного управління [63].

У межах дослідження безпеки систем електронного документообігу (СЕД) базовою категорією виступає поняття порушника. Йдеться про користувача, який реалізує або має намір провести несанкціоноване вторгнення, здобувши доступ до даних шляхом виявлення програмно-технічних чи організаційних проблем у стані захисного контуру підприємства. Стосовно сучасних установ потенційних порушників класифікують на так званих зовнішніх зловмисників (наприклад, хакерів чи

представників конкуруючих фірм) та внутрішніх зловмисників (працівників-інсайдерів, що здатні зловживати наданими повноваженнями або ж дії яких викликані службовою недбалістю) [7]. Сама по собі загроза несанкційонованого доступу розцінюється як подія, що є наміром конкретної особи здійснити неправомірні спроби вторгнення до певної ділянки знаходження даних в інформаційній системі. Потенційні загрози неофіційного, несанкційонованого доступу до відомостей в інформаційних системах класифікують на:

1) цілеспрямовані, завідомо навмисні спроби вторгнення;

2) випадкового характеру, спричинені помилковими діями персоналу.

Випадкові загрози виникають незалежно від волі зловмисника і зумовлені технічними збоями обладнання, помилками у програмному забезпеченні СЕД або помилковими діями персоналу (скажімо, випадкове видалення діловодом важливої папки з договорами). Натомість цілеспрямовані (умисні) загрози є результатом свідомих дій порушника, спрямованих на заподіяння шкоди підприємству. Сучасна специфіка кіберзлочинності полягає в тому, що умисні загрози можуть маскуватися під випадкові шляхом довгочасної масованої атаки несанкційонованими запитами або комп'ютерними вірусами [1]. Наприклад, зловмисник може умисно перевантажити головний сервер запитами, щоб викликати його апаратне перезавантаження, і в момент технічного збою обійти систему автентифікації для викрадення цифрових архівів документів.

Залежно від цілей порушника, характерними різновидами такого роду неправомірних дій під час інформаційної діяльності на підприємстві є:

– проведення процесу ознайомлення з конфіденційними даними різноманітними способами, але без порушень їх структури та цілісності (копіювання файлів комерційних угод, клієнтських баз чи персональних даних на флешнакопичувачі або відправка їх на зовнішню пошту);

– зміна інформації з незаконною метою або як часткова чи загальна модифікація її складу (несанкційонована зміна банківських реквізитів у

платіжних документах, підробка цифрових резолюцій вищого керівництва, зміна умов контрактів);

– цілеспрямоване знищення даних задля завдання матеріальних збитків компанії (безповоротне видалення баз даних документів без можливості їх швидкого відновлення) [1].

Наслідком неправомірних дій з даними стає порушення їх конфіденційного характеру, повноти, достовірності фактажу та доступності, що у кінцевому результаті спричиняє порушення як самого режиму управління інформацією, так і його якісного боку за умов спотворення даних або ж їх неповноти. Керівництво та аналітики компанії в умовах роботи зі спотвореною інформацією втрачають можливість приймати адекватні управлінські рішення, що веде до значних фінансових втрат, зриву контрактів та юридичних санкцій [57].

Організація ефективного захисту від усього спектра виявлених умисних і випадкових ризиків вимагає обов’язкового переходу до етапу практичного проєктування та впровадження комплексних програмно-апаратних засобів на рівні конкретного підприємства.

Висновки до розділу 2

1) Урегулювання комплексу проблем, пов'язаних із тривалим архівним збереженням цифрових масивів документів, можливе лише за умови консолідації технологічних, міждержавних та нормативних важелів. Цілеспрямоване фінансування процесів стандартизації, розбудови відкритих форматів (зокрема PDF/A) та інструментів кібербезпеки дозволить гарантувати цілісність і спадковість електронної документації в сучасному інформаційному просторі.

2) Побудова надійного контуру захисту цифрових архівів не може обмежуватися лише встановленням антивірусного софту, а вимагає впровадження суворої системи резервування даних за принципом «3-2-1» та обов’язкової ізоляції внутрішніх підмереж установи. Організація ефективної

протидії Ransomware-атакам потребує детальної класифікації всіх векторів неправомірних дій, що актуалізує необхідність системного моделювання загроз та формування профілю потенційного порушника.

3) Розроблена модель загроз та порушника наочно доводить, що система електронного документообігу ТОВ «ІнфоТех-Консалтинг» потребує негайного впровадження адекватних інструментів захисту. Для нейтралізації умисних дій порушників та мінімізації наслідків технічних збоїв, у наступному розділі роботи буде запропоновано комплекс програмно-апаратних, криптографічних та технічних рішень.

РОЗДІЛ 3.
ПРАКТИЧНІ АСПЕКТИ ТА ТЕХНОЛОГІЇ ВПРОВАДЖЕННЯ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ: (НА ПРИКЛАДІ СЕД ТОВ «ІНФОТЕХ-КОНСАЛТИНГ»)

3.1. Загальна характеристика та моніторинг уразливостей IT-інфраструктури ТОВ «ІнфоТех-Консалтинг»

Здійснення практичного проєктування засобів захисту відомостей вимагає детального аналізу функціонування конкретної установи, визначення специфіки її документообігу та виявлення слабких місць у наявних управлінських процесах [5, с. 42]. Ефективність функціонування будь-якого сучасного суб'єкта господарювання в умовах цифровізації безпосередньо залежить від рівня автоматизації його бізнес-процесів та надійності оброблення управлінських даних.

Об'єктом прикладного ракурсу дослідження у цій роботі виступає товариство з обмеженою відповідальністю «ІнфоТех-Консалтинг» (ТОВ «ІнфоТех-Консалтинг»). Вказана організація є діючим суб'єктом господарювання в Україні, головним напрямом інформаційної та комерційної діяльності якого окреслюється надання висококваліфікованих юридичних, фінансових, аудиторських та комплексних консалтингових послуг для бізнесових структур [37].

Специфіка діяльності згаданої компанії зумовлює реалізацію поточного оперування практично на щоденній основі великою кількістю персональних даних клієнтів підприємства, звітними матеріалами фінансового характеру, корпоративними документами внутрішнього спрямування, що призводить до необхідності налаштування захищеної системи автоматизації основних процесів та організації належного комплексного захисту.

Задля обов'язкового дотримання комерційної таємниці, захищеності конфіденційних даних ТОВ «ІнфоТех-Консалтинг» та урахування чинних вимог політики корпоративної безпеки організації, у рамках нашого

дослідження з’явилася необхідність реалізації моделювання та знеособлення її точних мережевих характеристик. Відповідно до цього реально діючий технічний контур автоматизації та діловодної служби компанії у кваліфікаційній праці вивчається та описується у вигляді гіпотетичного, узагальненого обчислювального центру фірми. Подібний підхід дає можливість всебічно оцінити можливі організаційні й кадрові ризики та пробемні аспекти інформаційного менеджменту підприємства, не розголошуючи при цьому діючих критичних уразливостей її реальних серверних платформ [5].

Структура даного підприємства характеризується побудовою на підставі лінійно-функціонального принципу організації і включає такі базові управлінські й аналітичні ланки:

1) очільника (генерального директора);
2) юридичний департамент;
3) фінансово-аудиторський підрозділ;
4) службу управління кадровим складом;
5) канцелярію (відділ діловодства);
6) ІТ-підрозділ (сектор технічного забезпечення інформаційної діяльності).

Щоденна інформаційна діяльність ТОВ «ІнфоТех-Консалтинг» супроводжується генеруванням та обробленням значних масивів конфіденційних та комерційно цінних документів. До них належать угоди з клієнтами, реєстраційні картки контрагентів, аудиторські звіти, стратегічні бізнес-плани розвитку замовників, фінансова звітність компанії, а також накази з кадрових та операційних питань. Обмін вказаними документами як усередині фірми, так і з зовнішніми партнерами, здійснюється із активним використанням хмарного сервісу «Вчасно» та елементів автоматизованої системи електронного документообігу «Megapolis.DocNet».

Вивчення стану інформаційної роботи ТОВ «ІнфоТех-Консалтинг» дозволило з’ясувати, що середньорічний обсяг документообігу компанії

умовно дорівнює близько 15 тис. одиницям управлінських та комерційних документів. З метою побудови раціональної та якісної системи захисту та оптимізації кадрових повноважень, автором було здійснено типологізацію документаційних потоків установи за трьома основними режимами доступу відповідно до норм Закону України «Про інформацію» [47]:

- конфіденційна інформація підприємства, тобто комерційна інформація підприємства (аудиторські звіти, клієнтські бази даних, стратегічні фінансові плани, тексти угод із замовниками консалтингових послуг);
- службова інформація, що стосується внутрішнього документообігу (кадрові накази дирекції, штатні розклади, бухгалтерські відомості, протоколи внутрішніх нарад, номенклатура справ канцелярії);
- відкрита інформація, що знаходиться в публічному доступі (пресрелізи, маркетингові пропозиції компанії, загальна інформація про послуги на корпоративному вебсайті).

Проведене аналітичне обстеження умовного обчислювального центру та діловодних процесів ТОВ «ІнфоТех-Консалтинг» дозволило ідентифікувати низку можливих організаційних, кадрових та технічних уразливостей захисного контуру підприємства:

1. Організаційно-управлінські недоліки. Очільником підприємства тривалий час недооцінювалася потреба у розробленні чіткої внутрішньої Політики інформаційної безпеки. В установі відсутні затверджені інструкції щодо поводження з конфіденційними цифровими архівами, а контроль за пересиланням управлінських файлів через відкриті публічні месенджери та особисту пошту працівників практично не здійснюється.

2. Кадрові ризики та вплив людського фактору. Результати обстеження вказують на низький рівень базової кібергігієни серед фахівців-аналітиків та менеджерів фірми. Досить розповсюдженою є практика фіксування автентифікаційних паролів до баз даних СЕД на звичайних паперових носіях, які зберігаються у відкритому доступі на робочих місцях

співробітників. Окрім того, встановлено факти передачі особистих флешносіїв із КЕП іншим працівникам канцелярії задля прискореного підписання наказів, що повністю нівелює принцип персональної юридичної відповідальності посадової особи.

3. Монополізування критичних функцій. Найбільш серйозною технічною та кадровою уразливістю умовного обчислювального центру фірми може бути концентрування всіх актуальних адміністративних паролів, доступів до серверів Active Directory, логів журналів аудиту та основних налаштувань безпеки в руках однієї єдиної особи – системного адміністратора. Брак дублювання функцій та взаємоконтролю створює загрози внутрішньої відмови виконання власних повноважень працівниками, шантажу керівництва або ж приховування фактів неправомірного доступу до комерційної таємниці організації.

4. Уразливі ділянки інфраструктури доступу. На підприємстві діє спрощений алгоритм допусків для вищого керівництва. Намагання топменеджерів компанії тримати безперешкодний і надшвидкий доступ до будь-яких баз даних документів, минуючи проходження процедур двофакторної автентифікації, створює ідеальну мішень для провадження зловмисниками зовнішніх фішингових атак та несанкціонованого проникнення у корпоративне середовище підприємства.

Отже, отримані результати обстеження переконують у тому, що існуючий рівень стану безпеки інформаційної роботи фірми не відповідає останнім вимогам щодо організації надійного кіберзахисту, а встановлені системні уразливості створюють сприятливе середовище задля безперешкодного проникнення програмних продуктів-вимагачів (наприклад, Ransomware) або втрати конфіденційних клієнтських масивів даних.

Нейтралізація виявлених організаційних та кадрових ризиків вимагає термінового переходу до детального аналізу стану наявного апаратно-програмного контуру, що і буде реалізовано у наступному підрозділі роботи.

3.2. Аналіз стану апаратно-програмного забезпечення безпеки інформаційної діяльності ТОВ «ІнфоТех-Консалтинг»

Основою системи управління та координації діяльності персоналу ТОВ «ІнфоТех-Консалтинг» є впроваджена система електронного документообігу (СЕД), яка забезпечує повний життєвий цикл документів. На базі СЕД функціонує електронна номенклатура справ організації, де права доступу розподілені за категоріями електронних папок відповідно до посадових обов'язків працівників [21].

Апаратно-технічний фундамент інформаційної інфраструктури компанії становить власний обчислювальний центр (так звана серверна кімната), який забезпечує працездатність корпоративної мережі. Архітектура телекомунікаційної системи підприємства побудована за клієнт-серверною моделлю в межах операційного середовища Windows Server і включає такі ключові компоненти, як:

– головний сервер баз даних СЕД;

– файловий сервер зберігання тіл цифрових документів (договорів, звітів);

– сервер автентифікації облікових записів співробітників Active Directory;

– комутаційне обладнання з маршрутизатором ядра мережі.

Фізично обчислювальний центр розташований у спеціально виділеному ізольованому приміщенні в межах центрального офісу підприємства. Процес обігу інформації в системі ЕДО ТОВ «ІнфоТех-Консалтинг» складається з трьох послідовних технологічних етапів [22]:

1) введення даних (сканування паперових носіїв, первинна реєстрація);
2) оброблення (маршрутизація документа всередині компанії, накладання КЕП);
3) виведення або архівування.

Кожен із цих етапів є вразливою ділянкою, де цифрові дані піддаються ризикам технічних збоїв або зловмисного втручання.

Детальний аналіз діючого програмно-технічного контуру дозволив виділити такі особливості наявного апаратно-програмного забезпечення установи:

1. Програмно-технічні засоби ідентифікації сесій. Права доступу користувачів, які безпосередньо працюють з цифровими архівами компанії, адмініструються на рівні локальних сертифікатів безпеки. Проте технічна верифікація сесій обмежена лише введенням статичних паролів до баз даних СЕД, що суттєво підвищує ризики компрометації облікових записів та вимагає впровадження превентивних інструментів захисту даних.

2. Конфігурація безпеки каталогів Active Directory. На аналізованому підприємстві в межах операційної системи зафіксовано технічну концентрацію повноважень з управління логами журналів безпеки та резервного копіювання в руках єдиного профілю – старшого системного адміністратора. З технічного боку, архітектура СЕД «Megapolis.DocNet» підтримує аудит дій користувачів, проте відсутність автоматизованого налаштування дублювання логів на незалежні апаратні носії створює ризик несанкційонованого видалення технічних записів у разі виникнення внутрішніх інцидентів.

3. Технічний контроль зовнішніх підключень. Частина робіт із технічного обслуговування обчислювального центру та оновлення модулів СЕД покладена на аутсорсингову організацію. Програмний контроль за діями цих сторонніх осіб під час їхнього віддаленого підключення за допомогою протоколів віддаленого робочого столу (RDP) є недостатнім. У локальній мережі не реалізовано автоматичне відеофіксування або суворе шифрування сесій, що створює ризик несанкційонованого копіювання баз даних подвійного призначення чи приховування фактів порушення роботи центру.

Паралельно з програмно-мережевими чинниками, моніторинг апаратного контуру умовного обчислювального центру виявив суттєві

інженерно-технічні та природно-техногенні ризики. Незважаючи на фізичну ізольованість серверної кімнати, на об'єкті наразі повністю відсутнє автоматизоване обладнання виявлення і гасіння пожежі, устаткування виявлення витоків води, а також не впроваджено конструкційні заходи захисту від розкрадань, саботажу чи диверсій. Приміщення обчислювального центру потребує термінового встановлення додаткових резервних систем безперебійного електроживлення (ДБЖ та дизель-генераторів), оснащення приміщень кодовими або біометричними замками та підключення сигналізації. За поточних умов будь-яка аварія систем опалення, затоплення або раптовий збій у загальній електромережі будівлі може призвести до повного фізичного руйнування апаратного комплексу та безповоротної втрати баз даних цифрових архівів компанії.

3.3. Напрямки модернізації системи захисту документаційної діяльності та перспективи автоматизації електронного документообігу підприємства

На основі результатів аналізу уразливостей інформаційної діяльності та процесів діловодства в ТОВ «ІнфоТех-Консалтинг» було проведено комплексний аналіз стану апаратно-програмного забезпечення та розроблено проєкт переоснащення системи електронного документообігу (СЕД) компанії.

Оскільки в сучасній інформаційній діяльності вже неможливо тримати всі масиви документів у голові або на паперових носіях, комп’ютерні технології та цифрові архіви мають стратегічну цінність для бізнесу. Проте паралельно з оптимізацією діловодства з’являється загроза несанкційонованого доступу до конфіденційних папок осіб, які не мають на це права, що вимагає впровадження надійних апаратно-програмних засобів контролю. Для організації переконливого захисту інформаційних ресурсів

безпосередньо в процесі документообігу ТОВ «ІнфоТех-Консалтинг» було реалізовано такі прикладні апаратно-програмні рішення:

1. Програмні засоби диференціації та розмежування прав доступу. На основі розробленої матриці повноважень у СЕД компанії було активовано модулі автоматичного контролю доступу. Для фахівців-документознавців це дозволило чітко розмежувати права користувачів під час формування електронної номенклатури справ. Система забезпечує відкритий доступ усім працівникам для ознайомлення з відкритою інформацією установи, але суворо блокує будь-які спроби несанкційонованої модифікації чи видалення файлів особами, які не мають відповідних повноважень. Доступ до комерційної таємниці та особистої конфіденційної інформації клієнтів надається виключно авторизованим аналітикам з можливістю оперативного надання чи позбавлення права на виконання конкретних операцій (читання, редагування, копіювання) [16].

2. Апаратно-програмний захист від витоків інформації (DLP-системи). Для захисту конфіденційної документованої інформації від внутрішніх порушників (інсайдерів) на робочих станціях персоналу розгорнуто програмний комплекс DLP (Data Loss Prevention). Система здійснює безперервний моніторинг інформаційної діяльності працівників та фізично унеможливлює спроби скопіювати будь-який службовий документ або клієнтську базу на зовнішній флешнакопичувач чи надіслати файл на особисту електронну пошту, месенджери та хмарні сховища, миттєво блокуючи неправомірні дії та ведучи захищений журнал реєстрації для подальшого аудиту діловодів.

3. Апаратне забезпечення цілісності та відмовостійкості цифрових архівів. Для надійного збереження інформаційних ресурсів ТОВ «ІнфоТех-Консалтинг» у разі порушення працездатності окремих технічних ланок, архітектуру мережі перепроєктовано за принципом перерозподілу ресурсів. Серверний парк зберігання електронних архівів оснащено технологією апаратного резервування критичних підсистем та жорстких дисків у

поєднанні з автоматизованим щоденним бекапом даних. Це гарантує точність і повноту інформації, захищаючи цифрові архіви від випадкового або умисного руйнування та знищення внаслідок збоїв, саботажу чи вірусних атак [17].

4. Захист документаційних потоків у каналах зв'язку. Оскільки інформаційна діяльність підприємства передбачає постійний обмін електронними документами з віддаленими філіями та клієнтами, відкрита передача повідомлень по відкритих мережах є неприпустимою. Замість побудови складних ізольованих ліній, у ТОВ «ІнфоТех-Консалтинг» реалізовано технологію передачі повідомлень по відкритому каналу Інтернет, але лише після спеціального перетворення шифрування. Це унеможливлює отримання корисної інформації про зміст управлінського документа сторонньою особою під час його транспортування мережею без знання спеціальної ключової інформації – секретного ключа [14].

Урахування теоретичних засад захисту інформаційних ресурсів у практичній діяльності ТОВ «ІнфоТех-Консалтинг» дозволило надати електронному документообігу компанії повноцінної юридичної сили, рівнозначної власноручному підпису та мокрій печатці установи. На базі використання діловодних систем «Megapolis.DocNet» та сервісу «Вчасно» на підприємстві реалізовано покроковий технологічний алгоритм застосування Кваліфікованого електронного підпису (КЕП).

Діловод або уповноважений аналітик фірми здійснює підписання управлінських документів за допомогою особистого закритого ключа, який фізично зберігається на захищеному апаратному носії (USB-токені). При цьому інтегровані модулі СЕД автоматично взаємодіють із серверами кваліфікованого надавача довірчих послуг, генеруючи не лише зашифрований дайджест файлу, а й обов'язкову позначку часу (Time Stamp), що гарантує валідність документа в цифровому архіві навіть після завершення терміну дії сертифіката працівника.

Впровадження організаційних регламентів та Плану аварійного відновлення (DRP) зумовлює дотримання ряду вимог. Для забезпечення надійної працездатності СЕД у разі виникнення технічних збоїв, саботажу чи успішних вірусних атак типу Ransomware, для ТОВ «ІнфоТех-Консалтинг» було розроблено та використано прикладний План аварійного відновлення (Disaster Recovery Plan – DRP) [15]. Цей регламент чітко розподіляє комплекс зобов’язань та відповідальність між ІТ-персоналом та діловодними службами установи:

1. Графік створення копій. Бази даних СЕД та електронні документи автоматично копіюються за «правилом 3-2-1» (створення трьох копій на двох різних типах носіїв із обов’язковим винесенням однієї копії на хмарний сервер поза межами офісу компанії).

2. Алгоритм дій при зараженні. У разі виявлення на робочій станції працівника перших ознак роботи вірусної програми-вимагача (раптова зміна розширень файлів, блокування інтерфейсу), посадова особа зобов'язана негайно відключити комп’ютер від локального мережевого контуру. Це повністю запобігає поширенню шкідливого коду на головні сервери СЕД та довгострокові цифрові архіви компанії, усуваючи ризик тотального паралічу операційного управління.

Результати проведеного раніше обстеження уразливостей вимагали негайного перегляду організаційних методів захисту корпоративного середовища ТОВ «ІнфоТех-Консалтинг». З метою ліквідації кадрових ризиків на підприємстві було реалізовано такі адміністративні рішення:

– принцип універсальності засобів захисту (скасовано практику спрощеного доступу до СЕД для вищого керівництва фірми). Топменеджери компанії переведені на загальні правила безпеки з обов’язковим використанням двофакторного рівня автентифікації та КЕП, що повністю нівелювало ризики успішного застосування фішингових атак проти облікових записів керівництва установи;

– регламентація підбору кадрового складу (до посадових інструкцій служби управління персоналом внесено обов’язкову вимогу щодо проведення поглибленої перевірки професійної надійності та дотримання правил конфіденційності новими працівниками при прийомі на роботу;

– розподіл критичних функцій (повністю ліквідовано уразливість «монополізації робіт» однією людиною)

Всі обов’язки з адміністрування баз даних СЕД та керування логами журналів аудиту відтепер дублюються між двома незалежними фахівцями, що цілком виключає загрози внутрішнього саботажу, шантажу чи приховування фактів несанкційонованого доступу до відомостей суб’єктами господарювання.

Технічні перспективи розвитку електронного урядування на підприємстві передбачають урахування декількох важливих факторів. Аналіз тенденцій розвитку інформаційних технологій дозволяє визначити ключові орієнтири модернізації системи ТОВ «ІнфоТех-Консалтинг» на довгострокову перспективу.

По-перше, актуальним є перехід до хмарних захищених довірчих послуг (Cloud-КЕП). Зокрема, перспективним кроком стає повна відмова від фізичних носіїв ключової інформації співробітників на користь технологій дистанційного підписання управлінських документів (наприклад, інтеграція СЕД із хмарними сховищами сертифікатів або системою «Дія.Підпис»), що повністю ліквідує ризики втрати, пошкодження чи фізичної крадіжки носія ключа персоналом.

По-друге, нагальним завданням є впровадження алгоритмів штучного інтелекту (ШІ) у DLP-системи. Для надійного виключення людського фактора подальша модернізація передбачає впровадження модулів машинного навчання всередині DLP-комплексу. ШІ здатний аналізувати інформаційну діяльність діловодів у реальному часі, виявляти аномальну поведінку користувачів та автоматично блокувати випадкові помилки

персоналу (наприклад, спробу помилкового надсилання конфіденційного файлу сторонньому адресату) ще до моменту реалізації загрози витоку.

По-третє, доцільним є проведення адаптації під концепцію «Privacy by Design» за стандартами GDPR. Євроінтеграційний курс вимагає автоматизації процесів знеособлення (анонімізації) персональних даних клієнтів в електронних архівах компанії при реалізації європейського права особи «бути забутим», без порушення цілісності номенклатури справ та збереження правової спадковості даних.

Висновки до розділу 3

1) Результати проведеного обстеження наявного стану безпеки ТОВ «ІнфоТех-Консалтинг» свідчать про високий рівень організаційних, кадрових та технічних ризиків. Без усунення виявлених уразливостей, зокрема без чіткого розмежування відповідальності осіб, регламентації роботи з кадровим складом персоналу, наявності плану відновлення працездатності обчислювального центру після збоїв та модернізації фізичного захисту приміщення – впровадження будь-яких програмних засобів безпеки не принесе бажаного теоретичного ефекту.

2) Проведений аналіз стану апаратно-програмного забезпечення інформаційної діяльності дозволив розробити прикладний проєкт модернізації, завдяки якому на підприємстві ТОВ «ІнфоТех-Консалтинг» сформовано надійний контур захисту СЕД. Поєднання систем контролю прав доступу, захисту від витоків DLP та технологій апаратного резервування дозволяє захистити інформаційну діяльність підприємства на всіх етапах обігу документів, мінімізуючи управлінські ризики роботи в умовах спотвореної або неповної інформації.

3) Вивчення напрямків модернізації системи захисту документаційної діяльності компанії доводить, що тільки комплексний підхід, який поєднує передові криптографічні алгоритми, постійне оновлення програмного середовища та високу кібергігієну фахівців-документознавців,

здатний гарантувати надійне збереження комерційних інформаційних ресурсів підприємства. Впровадження систем електронного документообігу є незворотним процесом, який значно підвищує якість операційного менеджменту. Однак довіра до цих систем прямо пропорційна рівню їхньої захищеності.

ВИСНОВКИ

За результатами дослідження відповідно до поставлених завдань зроблено наступні висновки:

1) Уточнено роль інформації як важливого стратегічного ресурсу та розкрито специфіку інформаційної сфери в умовах сучасного суспільства. Доведено, що в глобальному інформаційному соціумі інформація видозмінилася з інструменту додаткового засобу фіксації даних на цілком самостійний, незалежний та стратегічно необхідний продукт. Ефективна технологічна модернізація основних систем управління на базі ІТ-технологій сьогодні вимагає превентивного розвитку засобів захисту відомостей. Комплексна безпека інформаційного простору підприємства більше не зводиться до питання технічного захисту, оскільки виступає головною вимогою збереження його функціональної стабільності та виживання в мінливих ринкових умовах.

2) З’ясовано, що специфіка електронного документообігу як об’єкта захисту полягає у фізичній нематеріальності цифрового документа, який становить собою структурований набір двійкових даних. Організація захищеної інформаційної діяльності установ потребує одночасного забезпечення конфіденційності, цілісності та доступності даних, а також перевірки їхньої автентичності за допомогою криптографічних перетворень та інфраструктури довірчих послуг, без чого цифрові масиви втрачають юридичну силу.

3) Визначено принципи нормотворчості та завдання державних інституцій у сфері забезпечення інформаційної безпеки України. У державі створена дієва національна система правового регулювання, правову основу якої становлять Конституція України та Закони України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про державну таємницю» тощо. Однією з провідних регулюючих інституцій у напрямі координації та контролю захисту інформації є Держспецзв’язку, що

забезпечує формування Національної системи конфіденційного зв'язку (НСКЗ), яка є захищеною транспортною основою для обміну документацією. Разом з тим, виявлено правовий розрив між потребами хмарного діловодства та застарілими положеннями концепцій, що обґрунтовує потребу в прийнятті Інформаційного кодексу України.

4) Встановлено, що євроінтеграційні процеси та стандарти (GDPR) суттєво впливають на практику захисту даних в Україні. Сьогодні існує необхідність адаптації українських систем автоматизації бізнесу до вимог Загального регламенту про захист даних. Впровадження європейських принципів «Privacy by Design» та права особи «бути забутим» вимагає автоматизації процесів анонімного представлення персональних даних клієнтів в електронних архівах компаній, розгортання відкритих форматів довгострокового зберігання файлів (зокрема, PDF/A) та впровадження стандартів серії ДСТУ ISO/IEC 27001:2017.

5) Охарактеризовано типи сучасних вірусних загроз для цифрових архівів та класифіковано методи щодо їх подолання. Доведено, що найбільшу небезпеку для систем управління документами становлять програми-вимагачі (Ransomware) та масштабні умисні кібератаки шкідливого софту (наприклад, вірусу Petya/NotPetya), які здатні завуальовувати свої дії під випадкові апаратні проблеми та спричинити зупинку операційного управління. Ефективна протидія зазначеним ризикам передбачає чітке дотримання міжнародного «правила 3-2-1» стосовно створення резервних копій даних та розмежування внутрішньої, локальної інфраструктури підприємств.

6) Змодельовано загрози несанкційонованого доступу та визначено неправомірні дії із документованою інформацією. Сформовано умовний профіль потенційного порушника, який детально розподілено на зовнішнє (хакери, конкуренти) та внутрішнє середовище (представники кадрового персоналу установи). Класифіковано основні алгоритми неправомірних дій користувачів (несанкціоноване ознайомлення, часткова або загальна модифікація складу відомостей та цілеспрямоване знищення даних), що

дозволило встановити пряму залежність між захищеністю джерельної повноти й достовірності інформаційного середовища та якістю прийняття управлінських рішень.

7) Проведене оцінювання організаційних, кадрових та технічних вразливостей умовного обчислювального центру підприємства ТОВ «ІнфоТех-Консалтинг» (із середньорічним обсягом документаційних потоків близько 15 тис. одиниць та типологізацією папок за режимами доступу відповідно до норм закону). Ідентифіковано низку критичних ризиків: відсутність внутрішньої Політики безпеки, незадовільний стан кібергігієни кадрового складу (записування паролів, передача ключів електронного підпису), небезпечне зосередження всіх адміністративних допусків в руках однієї особи – системного адміністратора, а також природно-техногенні ризики серверної кімнати (повна відсутність автоматичного пожежогасіння та датчиків витоків води).

8) Проаналізовано стан апаратно-програмного забезпечення безпеки інформаційної діяльності ТОВ «ІнфоТех-Консалтинг». Встановлено, що архітектура телекомунікаційної системи побудована за клієнт-серверною моделлю в межах середовища Windows Server та каталогів Active Directory. Виявлено технічні недоліки чинного програмного середовища: перевірка сесій обмежена лише статичними паролями в базах даних, у системі відсутнє автоматичне дублювання логів журналів безпеки на незалежні апаратні носії, а програмний контроль за віддаленими підключеннями аутсорсингових фахівців за протоколами RDP є недостатнім через брак відеофіксації сесій.

9) Окреслено напрямки модернізації системи захисту документаційної діяльності підприємства. Впроваджений комплекс засобів охоплює автоматичне розмежування прав доступу користувачів у СЕД «Megapolis.DocNet» за регламентованим профілем допусків персоналу, розгортання захисного комплексу від внутрішніх витоків інформації (DLP-системи), технології апаратного резервування критичних підсистем та шифрування каналів зв’язку при взаємодії з хмарним сервісом «Вчасно».

Організаційний бік захисту інформації може бути надійно підкріплений затвердженням Плану аварійного відновлення (DRP), ліквідацією привілеїв доступу для вищого керівництва та дублюванням функцій адміністрування. Визначено, що довгостроковими орієнтирами розвитку електронного урядування на підприємстві є перехід до хмарних кваліфікованих електронних послуг («Дія.Підпис») та інтеграція в системи машинного навчання штучного інтелекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Аль-Амморі А. Н., Дехтяр М. М., Іщенко Р. М., Клочан А. Є. Методи та засоби захисту інформації. *Сучасні інформаційні системи*. 2024. Т. 8. № 1. С. 44–48.

2. Антоненко І. Є. Керування документацією за кордоном : історія, законодавство, теоретичні основи та технології : автореф. дис. … канд. іст. наук: 07.00.10. Київ, 2005. 20 с.

3. Антоненко І. Є. Стандартизація процесів управління документацією: досвід Австралії. Документознавство. Бібліотекознавство. Інформаційна діяльність : проблеми науки, освіти, практики: зб. матеріалів Міжнар. наук.-практ. конф. (Київ, 25–26 трав. 2004 р.). Київ, 2004. С. 60–62.

4. Бездрабко В. В. Документознавство в Україні: історія, сучасний стан і перспективи розвитку: монографія. Київ : Четверта хвиля, 2020. 284 с.

5. Бєляков К. І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення: монографія. Київ: КВІЦ, 2008. 576 с.

6. Бєляков К. І., Мірошник Ю. П. Проблеми законодавчого регулювання у сфері користування інформацією з обмеженим доступом в Україні. *Стратегічна панорама*. 2004. № 3. С. 171–177.

7. Бондаренко І. П. Антивірусні технології та методи захисту інформації. Харків: Основа, 2020. 312 с.

8. Босак І. Інформаційна безпека України: загрози та методи протидії. *Київський економічний науковий журнал*. 2025. № 9. С. 33–38.

9. Бурцева К. О. Захист конфіденційної інформації в мережі internet та соціальних мережах. Радіоелектроніка та молодь у XXI столітті : матеріали 28-го Міжнар. молодіж. форуму, 16–18 квітня 2024 р. Харків : ХНУРЕ, 2024. Т. 3. С. 465–466.

10. Вербіцький О. В. Вступ до криптології. Львів : ВНТЛ, 1998. 248 с.

11. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки : навч. посіб. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2020. 128 с.

12. Войцехівська І. Н. Криптографія. Енциклопедія історії України : у 10 т. / редкол.: В. А. Смолій (голова) та ін. ; Інститут історії України НАН України. Київ : Наукова думка, 2009. Т. 5: Кон – Кю. С. 390.

13. Голубовська В. С. Інформаційне суспільство: можливості, проблеми та перспективи розвитку. Інформація і право. 2013. № 2. С. 98-104. URL: http://nbuv.gov.ua/UJRN/Infpr_2013_2_14

14. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія : навч. посіб. Харків: ХНУРЕ, Форт, 2012. 878 с.

15. ДСТУ ISO/IEC 27001:2017. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013, IDT). Київ : ДП «УкрНДНЦ», 2017. 34 с.

16. ДСТУ ISO 15489-1:2018. Інформація та документація. Керування документами. Частина 1. Поняття та принципи (ISO 15489-1:2016, IDT). Київ: ДП «УкрНДНЦ», 2019. 34 с.

17. Єсін О.О., Кузнецов О.О., Сорока Л.С. Безпека інформаційних систем і технологій: Навч. посібник. Харків: ХНУ імені В. Н. Каразіна, 2013. 632 с.

18. Загальний регламент про захист даних (EU) 2016/679 (GDPR) / Європейський Парламент та Рада Європейського Союзу від 27 квітня 2016 р. Офіційний вісник Європейського Союзу. L 119. 2016. С. 1–88. URL: https://gdpr-text.com/uk/

19. Калужинська Ю. В., Троценко Р. В. Історія становлення документа та його еволюція в електронний документ. *Молодий вчений*. 2015. № 11(1). С. 71–74. URL: http://nbuv.gov.ua/UJRN/molv_2015_11%281%29__18

20. Кандирал Є. Застосування GDPR в Україні: аналіз кейсів вебсайт / Legal IT Group. URL: https://legalitgroup.com/zastosuvannya-gdpr-v-ukrayini-analiz-kejsiv/

21. Карпенко М.Ю. Електронний документообіг у професійній діяльності: конспект лекцій. Харків : ХНУМГ ім. О. М. Бекетова, 2020. 67 с.

22. Клименко І. В., Линьов К. О., Горбенко І. Д., Онопрієнко В. В. Електронний документообіг у державному управлінні: навч. посіб. Харків: ФОРТ, 2019. 232 с.

23. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч. посібник. Запоріжжя: НУ «Запорізька політехніка», 2020. 192 с.

24. Конах В. К. Нормативно-правові засади державної політики України у сфері інформаційно-психологічної безпеки. *Стратегічні пріоритети.* 2012. № 3 (24). С. 152–157.

25. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

26. Концепція технічного захисту інформації в Україні : затверджена Постановою Кабінету Міністрів України від 27.09.1997 № 1071. Офіційний вісник України. 1997. № 40. С. 39.

27. Кормич В. А. Правова регламентація інформаційної безпеки держави. Держава і право : зб. наук. пр. Юридичні і політичні науки. Вип. 17. Київ : Ін-т держави і права ім. В. М. Корецького НАН України, 2002. С. 193–198.

28. Криптографія // Літературознавча енциклопедія: у 2 т. / авт.-уклад. Ю. І. Ковалів. Київ : ВЦ «Академія», 2007. Т. 1 : А – Л. С. 532.

29. Кузнецов О. О., Євсеєв С. П., Король О. Г. Захист інформації в інформаційних системах. Методи традиційної криптографії: навчальний посібник. Харків : Вид. ХНЕУ, 2010. 316 с.

30. Кулешов С.Г. Електронний документ у системі сучасного діловодства. *Архіви України*. Київ, 2004. № 4/6. С. 50–53.

31. Кулешов С.Г. Управлінське документознавство: навч. посіб. Київ: ДАКККіМ, 2003. 57 с.

32. Матвієнко О. В., Цивін М. Н. Основи менеджменту інформаційних систем: навч. посіб. Київ: Центр навчальної літератури, 2005. 176 с.

33. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с.

34. НД ТЗІ 1.1-003-99. Термінологія у сфері технічного захисту інформації. Основні положення / Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України. Київ, 1999. 28 с.

35. Петрова С. В. Захист конфіденційної інформації та комерційної таємниці на підприємстві. Науковий вісник публічного та приватного права. 2021. Т. 2., № 5. С. 91–97.

36. Печериця Д. В., Чернов Д. В. Європейський регламент з охорони персональних даних. Прикладні аспекти сучасних міждисциплінарних досліджень : матеріали IV Міжнародної науково-практичної конференції (Вінниця, 10 квітня 2026 р.). Вінниця : ДНУ імені Василя Стуса, 2026. С. 168–170.

37. Плескач В. А., Затонацька Т. Г. Електронна комерція : підручник. Київ: Знання, 2007. 535 с.

38. Полотай О.І., Пузир А.О. Аналіз засобів запобігання витоку конфіденційної інформації на підприємствах на прикладі системи DLP. Львів. *Вісник ЛДУБЖД*. 2024. №30. С. 134–144.

39. Про Держспецзв'язку: вебсайт / Держспецзв'язку України. URL: https://cip.gov.ua/ua/statics/pro-derszhpeczv-yazku

40. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV. Відомості Верховної Ради України. 2006. № 30. Ст. 258. URL: https://zakon.rada.gov.ua/rada/show/n0055525-21#Text

41. Про Єдину державну інформаційну систему у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом,

і фінансуванню тероризму Постанова Кабінету Міністрів України від 10 груд. 2003 р. № 1896. Офіційний вісник України. 2003. № 51. С. 60. Стаття 2697.

42. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII. Відомості Верховної Ради України. 1994. № 16. Ст. 93. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

43. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. Відомості Верховної Ради України. 2017. № 45. Ст. 400. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

44. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV . Відомості Верховної Ради України. 2003. № 36. Ст. 276. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

45. Про затвердження Державної програми «Контрабанді — СТОП» на 2005–2006 роки : Постанова Кабінету Міністрів України від 01 квіт. 2005 р. № 260. URL: https://zakon.rada.gov.ua/go/260-2005-п

46. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994. №80/94-ВР. Відомості Верховної Ради України. 1994. № 31. Ст. 286.

47. Про інформацію : Закон України від 02.10.1992 № 2657-XII // Відомості Верховної Ради України. 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

48. Про науково-технічну інформацію : Закон України від 25.06.1993 № 3322-XII. Відомості Верховної Ради України. 1993. № 33. Ст. 345.

49. Про Національний архівний фонд та архівні установи : Закон України від 24.12.1993 № 3814-XII. Відомості Верховної Ради України. 1994. № 15. Ст. 86.

50. Про Національну систему конфіденційного зв’язку: Закон України від 10.01.2002 № 2913-III. Відомості Верховної Ради України. 2002. № 15. Ст. 103.

51. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. Відомості Верховної Ради України. 2018. № 31. Ст. 241.

52. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 09.01.2007 № 537-V. Відомості Верховної Ради України. 2007. № 12. Ст. 102.

53. Про Стратегію інформаційної безпеки : Указ Президента України від 28.12.2021 № 685/2021. Офіційний вісник України. 2022. № 4. Ст. 142.

54. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. Офіційний вісник України. 2021. № 68. Ст. 4305. URL: https://zakon.rada.gov.ua/rada/show/n0055525-21#Text

55. Рогова Є. І. Теоретичні основи правового забезпечення інформаційної безпеки. *Актуальні проблеми держави і права*. 2020. Вип. 86. С. 190–195.

56. Сакун Л. М., Буряк Є. В., Різніченко Л. В., Вєлькін Б. О. Управління стратегічними змінами операційної діяльності підприємства на засадах менеджменту бізнес-процесів. *Вісник Хмельницького національного університету*. Серія: «Економічні науки». 2021. № 6, Т.1. С. 73–79.

57. Семенюк Л. В. Ризики та наслідки втрати цілісності електронних документів в операційному менеджменті бізнес-структур. *Економіка та управління.* 2022. № 3. С. 67–73.

58. Ситник І. П., Мельниченко А. І. Системи електронного документообігу в електронному бізнесі. *Науковий вісник Ужгородського національного університету.* Серія: «Міжнародні економічні відносини та світове господарство». 2015. Вип. 4. С. 174–178.

59. Федотова О. О. Інформаційна політика ЄС із забезпечення безпеки діяльності користувачів в Інтернет-середовищі. Прикладні аспекти сучасних міждисциплінарних досліджень: матеріали III Міжнародної науково-практичної конференції (Вінниця, 1 листоп. 2024 р.). Вінниця : ДНУ імені Василя Стуса, 2024. С. 84–86.

60. Федотова О. О., Кудлай В. О. Місце інформаційних технологій у процесі забезпечення ефективного управління організаціями. Moderní aspekty vědy : LI. Díl mezinárodní kolektivní monografie / Mezinárodní Ekonomický Institut s.r.o. Česká republika : Mezinárodní Ekonomický Institut s.r.o., 2024. Str. 323–340. URL: https://repository.mu.edu.ua/jspui/bitstream/123456789/7988/1/Fedotova%20Kudlai%20mono.pdf

61. Харченко Л. С., Ліпкан В. А., Логінов О. В. Інформаційна безпека України: глосарій / за заг. ред. Р. А. Калюжного. Київ: Текст, 2004. 134 с.

62. Швецова-Водка Г. М. Документознавство: навч. посіб. Київ: Знання, 2007. 398 с. URL: https://duikt.edu.ua/uploads/l_1296_45107204.pdf

63. Юдін О. К., Новіков О. М. Захист інформації в інформаційно-комунікаційних системах: підручник. Київ: НАУ, 2020. 296 с.